WIRELESS 150N USB MINI ADAPTER USER MANUAL

MODEL 524773

INTELLINET™

NETWORK SOLUTIONS

INT-524773-UM-1009-01

Thank you for purchasing the INTELLINET NETWORK SOLUTIONS™ Wireless 150N USB Mini Adapter, Model 524773.

This ultra-compact high-speed adapter lets you connect your notebook or desktop PC to wireless networks faster than ever before, with link speeds of up to 150 Mbps. This adapter is also compatible with 802.11b and 802.11g wireless access points and wireless routers, giving you the flexibility to start upgrading your wireless network without the need to replace your existing equipment.

The easy-to-follow instructions in this user manual help make setup and operation relatively simple, so you'll soon be enjoying the benefits of these additional features:

- Supports WMM (Wi-Fi Multimedia) for increased multimedia data throughput
- Supports WEP (64/128 bit), WPA and WPA2 data encryption
- Supports Cisco CCX
- Supports the most popular operating systems: Windows XP, Vista and 7
- Supports Hi-Speed USB 2.0/1.1 interface
- Supports Software AP (turns your wireless client into a wireless access point)
- Lifetime Warranty

NOTE: For a quick install procedure, refer to the printed quick install guide enclosed with this product.

CONTENTS

1 INSTALLATION 5
1.1 Installing the Driver and Utility 5
1.2 Connecting to a Wireless Access Point 7
2 CONFIGURATION UTILITY 10
2.1 General 11
2.2 Profile 12
2.3 Available Network 16
2.4 Status 17
2.5 Statistics 18
2.6 Wi-Fi Protected Setup 18
2.6.1 Network Setup Using PIN Input Config 18
2.6.2 Network Setup Using Push Button Config 20
2.7 SoftAP 21
2.7.1 AP General / Properties Settings 21
2.7.2 AP Advanced 22
2.7.3 AP Statistics 24
2.7.4 ICS 24
3 SPECIFICATIONS 25

SAFETY & COMPLIANCE STATEMENTS

Federal Communications Commission (FCC) Statements

FCC PART 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of Federal Communications Commission (FCC) Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment *does* cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from the receiver.
- Consult the dealer or an experienced radio/TV technician for help.

FCC CAUTION

This device and its antenna must not be co-located or operated in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

FCC RADIATION EXPOSURE STATEMENT

This EUT complies with SAR for general population / uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and has been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C. The version marketed in the U.S. is restricted to usage of channels 1 through 11.

R&TTE Compliance Statement

This equipment complies with all the requirements of Directive 1999/5/EC of the European Parliament and the Council of March 9, 1999, on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE directive repeals and replaces Directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

SAFETY

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines must, therefore, be followed at all times to ensure the safe use of the equipment.

EU COUNTRIES INTENDED FOR USE

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU COUNTRIES NOT INTENDED FOR USE

None.

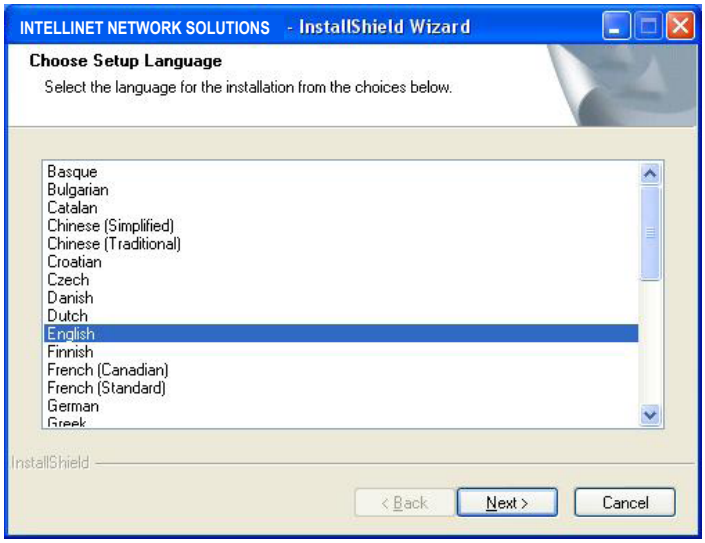
1 INSTALLATION

NOTE: The following installation represents Windows XP procedures and screen images, but both are similar for Windows 2000, Vista and 7. Some screen images have been modified to fit the format of this manual.

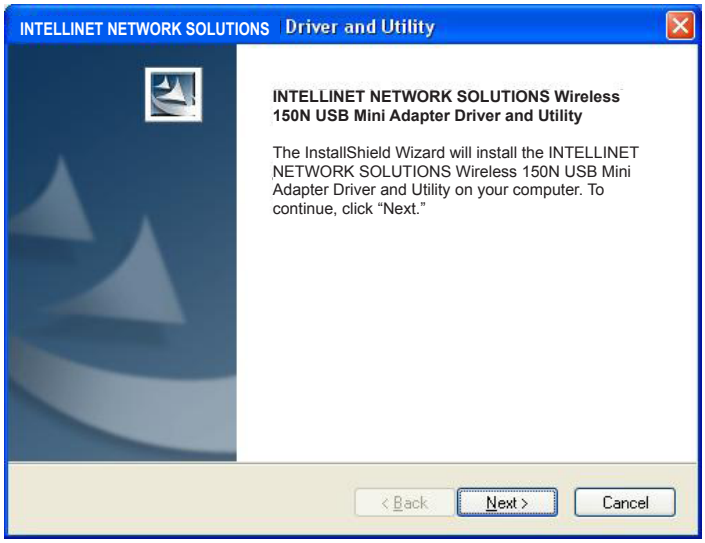
Prior to installation, un-install any previously installed versions of this adapter's driver or utility.

1.1 Installing the Driver and Utility

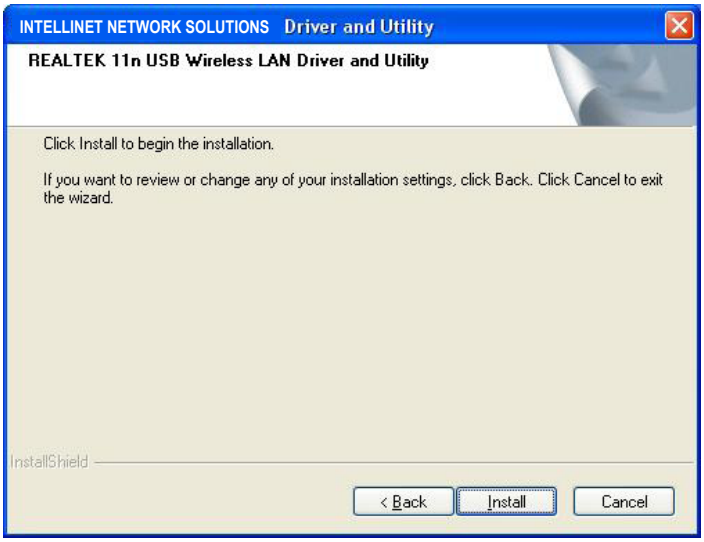
1. Insert the included setup/installation CD into your CD-ROM drive and run the "Setup.exe" program.
2. When the Choose Setup Language screen displays, highlight your preference and click "Next" to proceed.



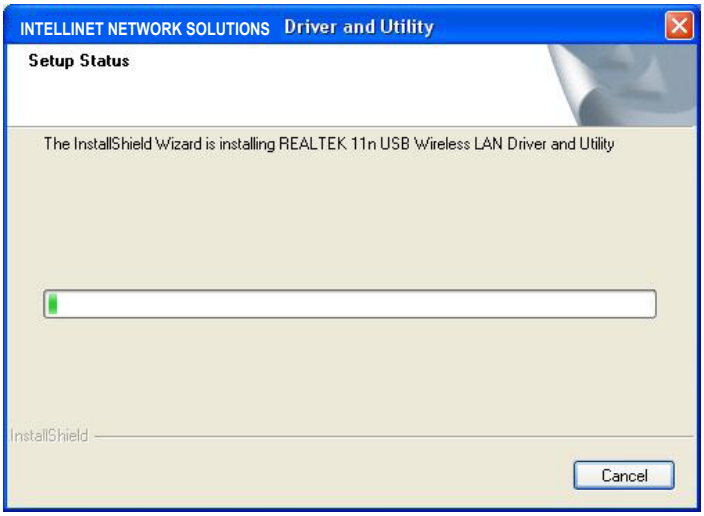
3. When the first of the Driver and Utility screens displays, click "Next."


INTELLINET NETWORK SOLUTIONS Driver and Utility
INTELLINET NETWORK SOLUTIONS Wireless 150N USB Mini Adapter Driver and Utility
The InstallShield Wizard will install the INTELLINET NETWORK SOLUTIONS Wireless 150N USB Mini Adapter Driver and Utility on your computer. To continue, click "Next."
< Back
Next >
Cancel

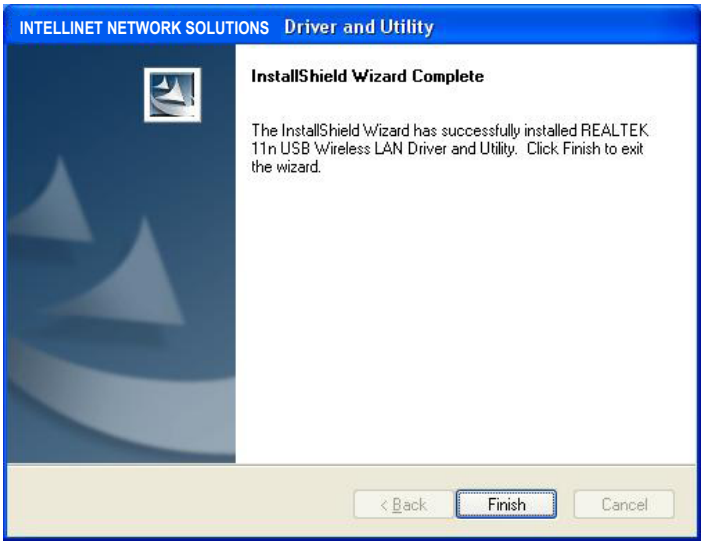
4. When the next screen displays, click “Install” to begin the installation. On any of the screens where they appear, click “Back” to return to a previous screen; click “Cancel” to exit the wizard.


INTELLINET NETWORK SOLUTIONS Driver and Utility
REALTEK 11n USB Wireless LAN Driver and Utility
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

5. The Setup Status screen will display, presenting a status bar that indicates the progress of the installation.

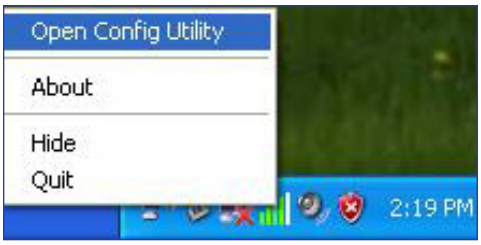

INTELLINET NETWORK SOLUTIONS Driver and Utility
Setup Status
The InstallShield Wizard is installing REALTEK 11n USB Wireless LAN Driver and Utility
InstallShield
Cancel

6. When the InstallShield Wizard Complete screen displays, click “Finish.”

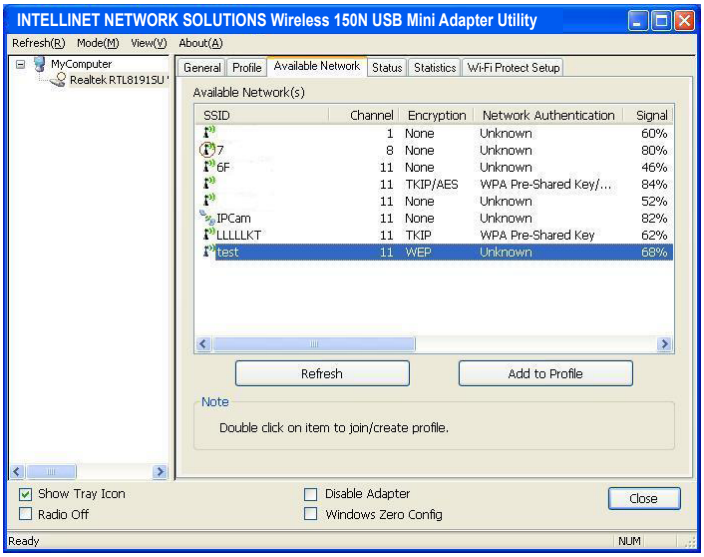

INTELLINET NETWORK SOLUTIONS Driver and Utility
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed REALTEK 11n USB Wireless LAN Driver and Utility. Click Finish to exit the wizard.
< Back
Finish
Cancel

1.2 Connecting to a Wireless Access Point

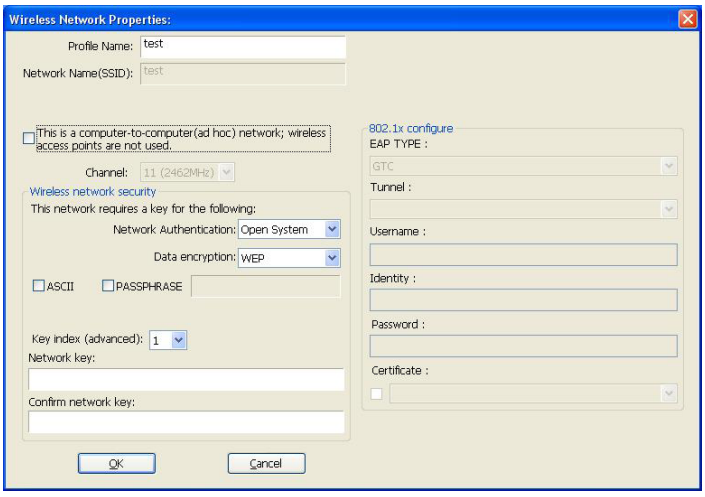
1. To begin the adapter configuration by connecting to a wireless AP, double-click the utility icon in the system tray (or right-click the one that automatically appears on the desktop), then select the “Open Config Utility” option from the popup menu.



2. When the Utility screen displays, click on the Available Network menu tab, then double-click the wireless access point you want to connect to from among those that appear in the Available Network(s) table, as shown at right.



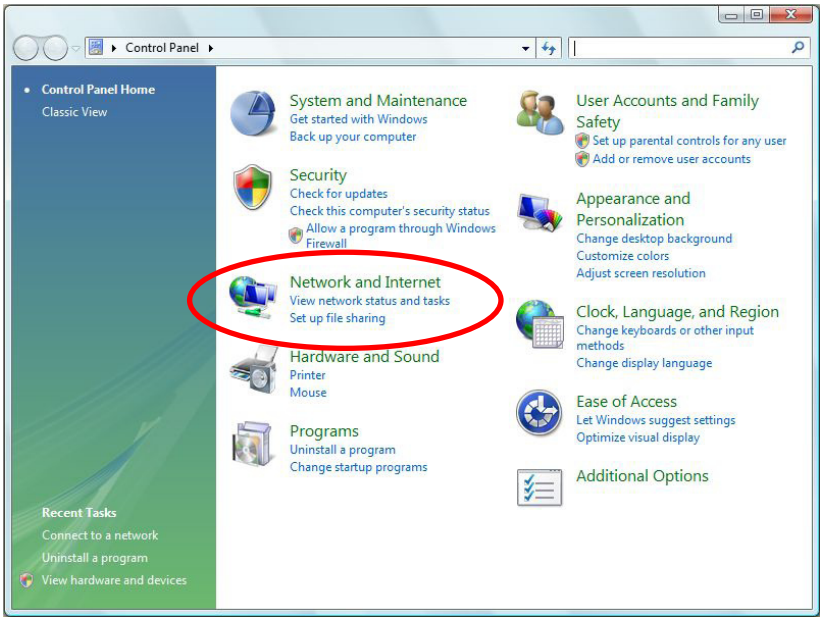
3. When the Wireless Network Properties screen displays, enter your security settings and click “OK” to initiate the network connection.



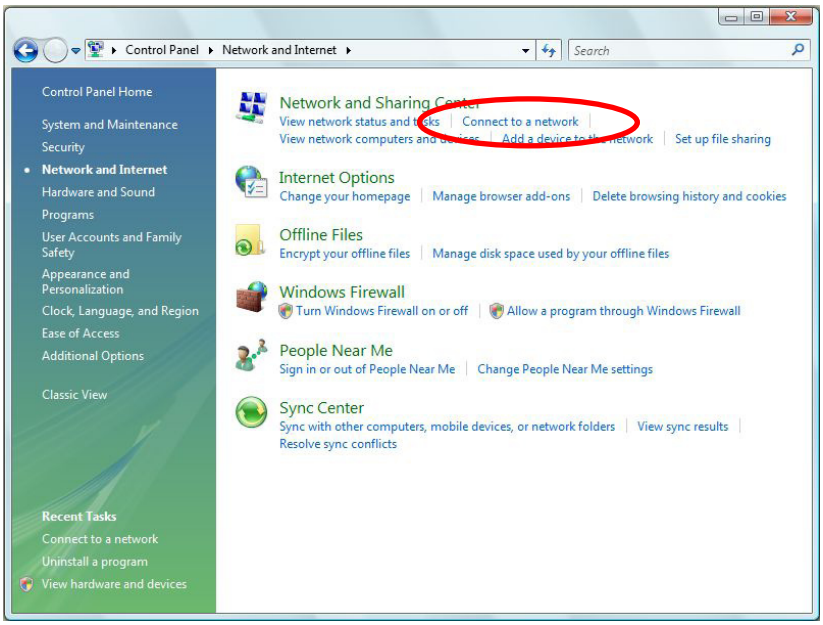
Windows Zero Configuration Option for Vista

Windows Vista users can connect to a wireless access point using the Windows Zero Configuration option.

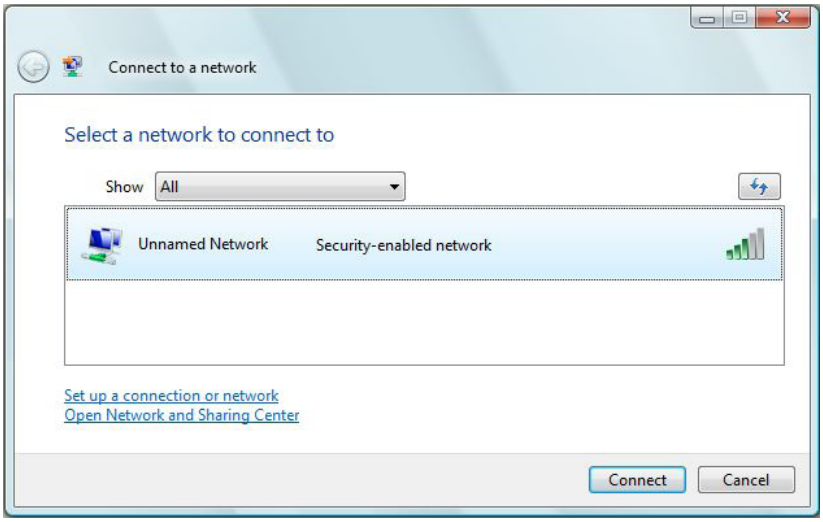
1. Go to Start, then Control Panel on the desktop, then select Network and Internet.



2. With the Network and Internet screen displayed, select “Connect to a network” under the Network and Sharing Center heading.



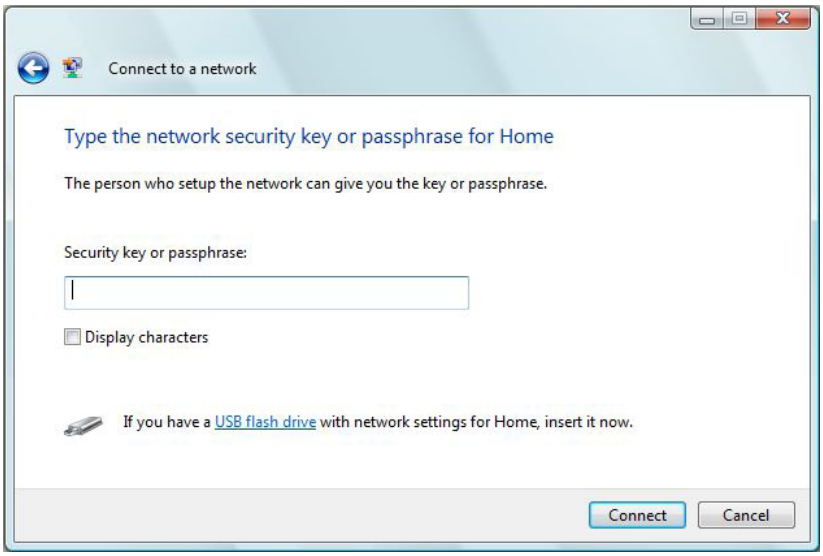
3. Highlight the access point you want to use (if it's shown), then click "Connect."



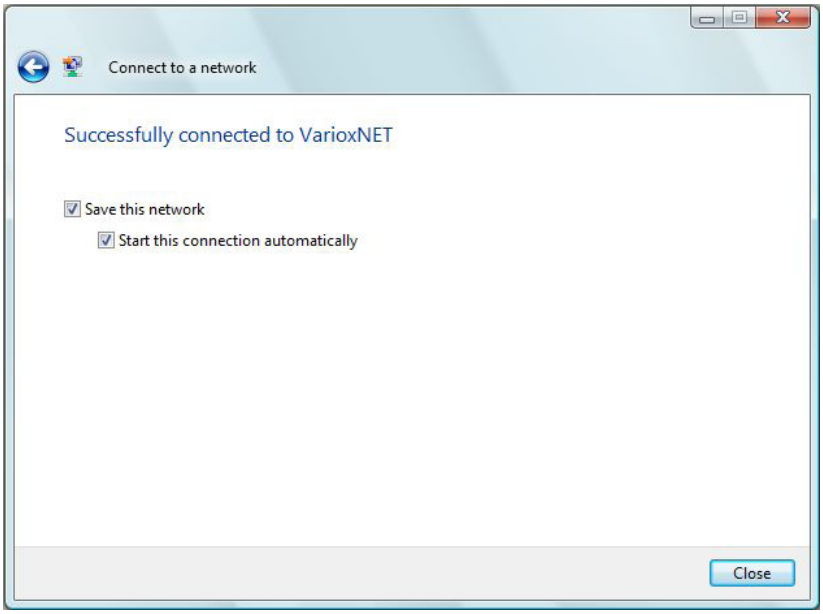
4. If it's an unnamed access point (i.e., the SSID of the wireless AP is hidden), you'll be prompted to input its name, which must be entered exactly — without error or deviation — in order to make a valid connection.

Connect to a network
Type the network name (SSID) for the network
Ask the person who set up this network to give you the name
Network Name:
Home
Next
Cancel

5. If the access point is protected by an encryption method, you need to input its security code or passphrase here. As with the SSID, it must match the encryption setting exactly. (Typically, you would obtain it from the AP's administrator.)

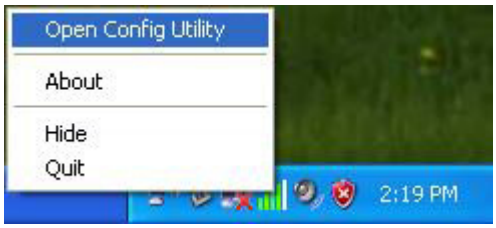

Connect to a network
Type the network security key or passphrase for Home
The person who setup the network can give you the key or passphrase.
Security key or passphrase:
Display characters
If you have a USB flash drive with network settings for Home, insert it now.
Connect
Cancel

6. Once the message “Successfully connected...” (between your computer and the wireless AP you selected) displays, click “Close” to start the network connection.



2 CONFIGURATION UTILITY

The Configuration Utility is a powerful application that helps you configure the Wireless 150N USB Mini Adapter and monitor the link status and the statistics during the communication process. The utility appears as an icon in the system tray and on the desktop of Windows. You can open it by double-clicking the desktop icon. Right-click the icon in the system tray and an options menu displays.



Above: utility system tray icon.
Right: utility options menu.

Open Config Utility: Select to open the configuration utility.
About: Select to display utility information.
Hide: Select to hide the utility in the system tray.
Quit: Select to quit the utility in the system tray.

The Configuration Utility opens to the General screen, with another five tabs near the top of the screen you can select for specific configuration options. Whichever of the tabs you select, several additional options are always displayed at the top, left and bottom of the screen, as shown on the General screen in the first of the detailed sections that follow.

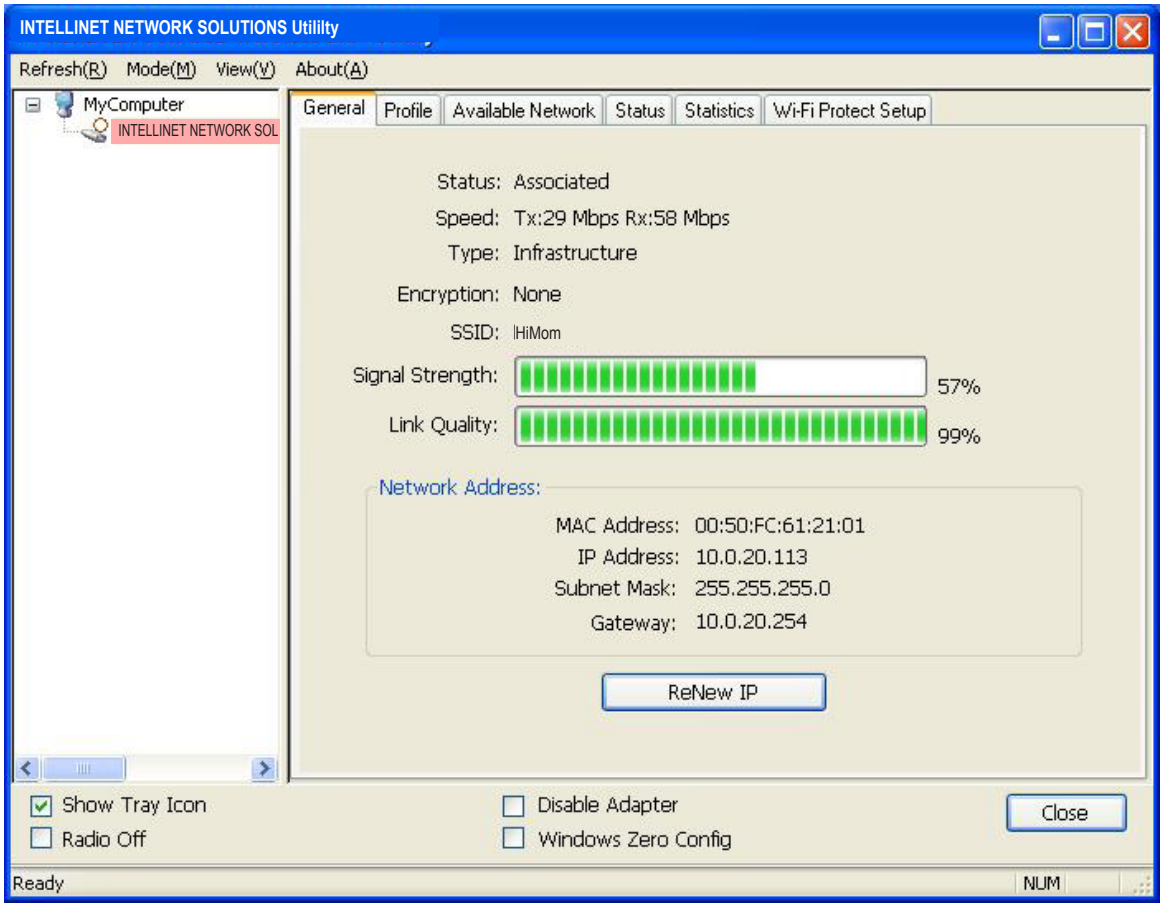
Refresh: This updates the adapter list in the left-side window.
Mode: This allows you to select one of two modes: Station or Access Point.

- With Station, the adapter works as a wireless adapter.
- With Access Point, the adapter works as a wireless AP. (See SoftAP.)

View: This allows you to enable “Status Bar,” which will display the current status of the utility at the bottom of the screen.
About: This lets you check the version of the utility.
Show Tray Icon: Select to show the utility icon in the system tray.
Radio Off: Select to turn off or turn on the radio of the adapter. If the radio is turned off, the adapter will not work.
Disable Adapter: This allows you to disable or enable the adapter.
Windows Zero Config: Select to configure the adapter using Windows XP Zero Configuration.

2.1 General

This screen is primarily for checking connection-related items and information about the selected adapter, some of which — Status, Speed, Signal Strength,



Link Quality and Network Address — are self-explanatory. The other references on this screen reflect the settings configured on the Profile screen.

Type: This displays either “Infrastructure” (operating in conjunction with an access point) or “Ad Hoc” (operating without an access point) based on the selection made on the Profile screen.

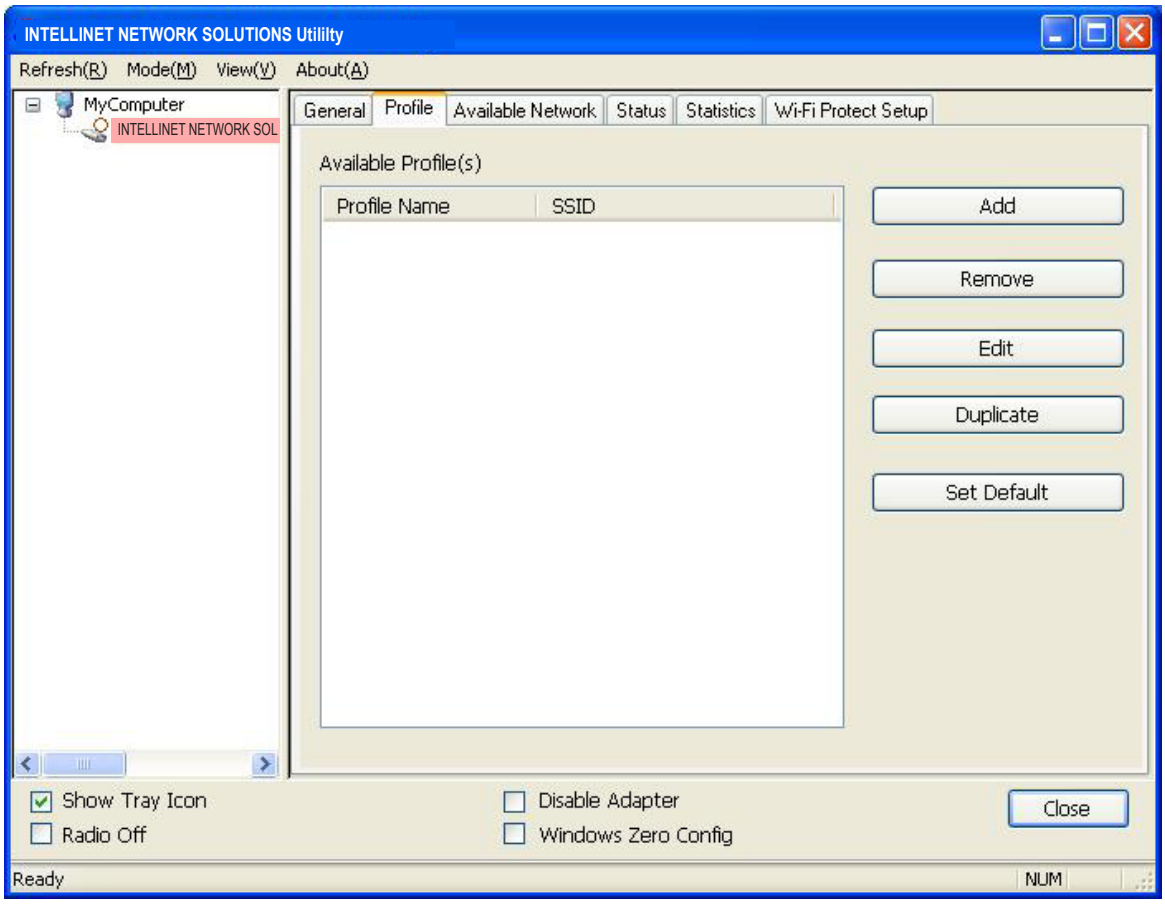
Encryption: This displays the encryption setting of the current connection — “None,” “WEP,” “TKIP” or “AES” — based on the selection made on the Profile screen.

SSID: The Service Set ID (up to 32 printable ASCII characters) is the unique name identified in a WLAN that prevents the unintentional merging of two co-located wireless networks. This can be entered on the Profile screen.

Renew IP: Click to renew the IP address of the adapter.

2.2 Profile

This screen helps you manage the networks you connect to frequently. By creating and using profiles, you can avoid the need to re-establish settings each time you make a connection.



Available Profile(s): This list shows the preferred networks for the wireless connection. You can add, remove, edit and duplicate the preferred networks, and you can also set one of the networks as the default connection.

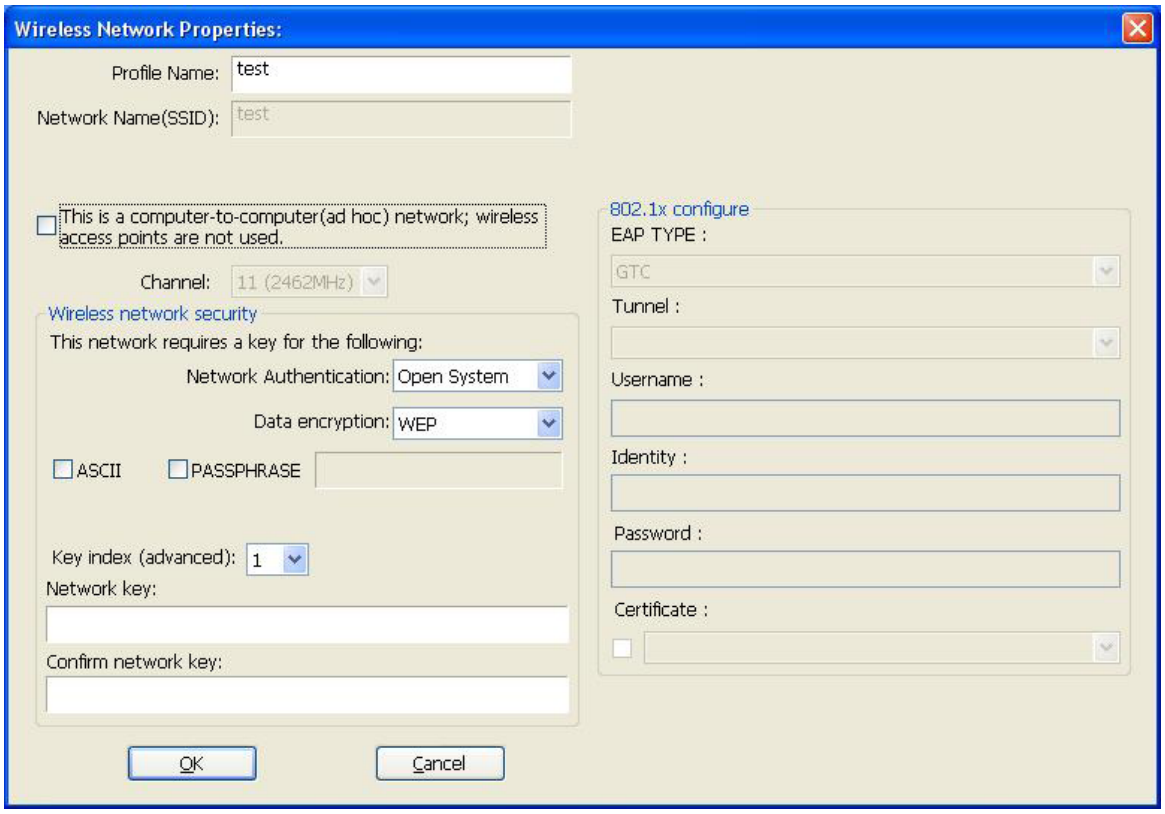
Add/Remove/Edit: Click with a profile selected to make desired changes.

Duplicate: Click to create a new profile with the same settings as the current one.

Set Default: Click to designate a selected profile on the Available Profile(s) list as the default network.

CONFIGURING A PROFILE

Clicking “Add” or “Edit” on the Profile screen will display a Wireless Network Properties screen that allows you to set various parameters required to be in synch with devices you connect to wirelessly.



Profile Name: Enter an easily recognizable name to quickly differentiate among multiple networks.

Network Name (SSID): The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. If you specify an SSID for the adapter, then only the device with the same SSID can connect to the adapter.

This is a computer-to-computer (ad hoc) network; wireless access points are not used.: When this option is selected, the adapter will operate in Ad Hoc

mode (connecting to another wireless adapter in the WLAN without an access point or router) vs. Infrastructure mode (which connects through an AP or router).

Channel: This setting is only available for Ad Hoc mode. Select the radio channel used for the network you're connecting to.

Network Authentication: This setting needs to be consistent with the wireless networks the adapter is intended to be connected to. There are seven options.

- Open System means that no authentication is needed within the wireless network.
- Shared Key means that only wireless stations using a shared key (WEP Key identified) are allowed to connect to each other.
- WPA-PSK is a special mode designed for home and small business users who don't have access to network authentication servers. In this mode, also known as Pre-Shared Key, the user manually enters the starting password in her access point or gateway, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users who don't have the matching password from joining the network while encrypting the data traveling between authorized devices.
- WPA2-PSK is also for homes and small businesses. It differs from WPA-PSK in that it provides data encryption via the Advanced Encryption Standard (AES). In contrast, WPA-PSK uses the Temporal Key Integrity Protocol (TKIP).
- WPA 802.1X (or just WPA) provides a scheme of mutual authentication using either IEEE 802.1x / Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. It provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.
- WPA2 802.1X, like WPA, supports IEEE 802.1x / EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required for corporate and government users. The difference between WPA and WPA2 is that WPA2 provides data encryption via the AES, whereas WPA uses the Temporal Key Integrity Protocol (TKIP).
- WEP 802.1X is a special mode for using IEEE 802.1x / EAP technology for authentication and WEP keys for data encryption.

Data Encryption: All devices in the network should use the same encryption method. The drop-down menu offers four options.

- Disabled disables the WEP data encryption.
- WEP enables the WEP data encryption. When this is selected, you need to continue with the setting of the WEP encryption keys.

- TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets. (A packet is a kind of message transmitted over a network.) This ensures much greater security than standard WEP security.
- AES has been developed to ensure the highest degree of security and authenticity for digital information. It's the most advanced solution defined by IEEE 802.11i for security in the wireless network.

ASCII / PASSPHRASE: WEP key entries can be in ASCII or passphrase format.

- ASCII uses alphanumeric values or signs, making it more easily recognizable for users.
- PASSPHRASE entries require a text string with a maximum of 32 alphanumeric characters; for example, "Test." The same passphrase or WEP key settings must be used for all wireless computers within the network. **NOTE:** Due to possible incompatibility with other manufacturers' passphrase generators, a passphrase may not work with other product brands.

Key Length: When "WEP" and "PASSPHRASE" are selected, this option displays.

- 64-bit lets you input 10-digit hexadecimal values as the encryption keys; for example, "0123456aef."
- 128-bit lets you input 26-digit hexadecimal values as the encryption keys; for example, "01234567890123456789abcdef."

Key Index (advanced): Select one of the four keys to be the data encryption key.

Network Key: Enter the network security key here to make sure the password is correct.

Confirm Network Key: Enter the network security key again.

EAP Type: The Extensible Authentication Protocol drop-down menu offers four options.

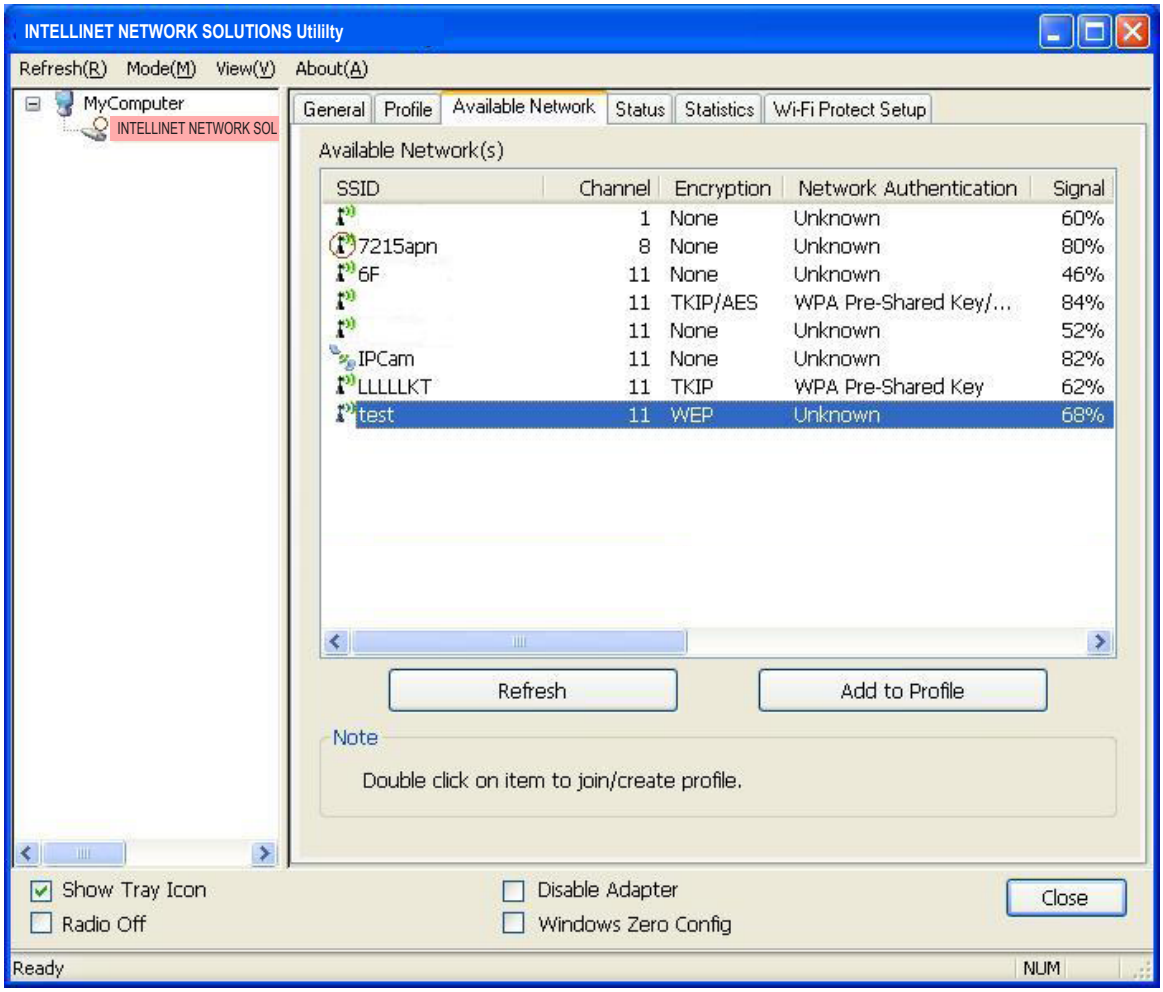
- GTC is an authentication protocol that allows the exchange of clear text authentication credentials across the network.
- TLS is the most secure of the EAP protocols, but isn't easy to use. It requires that digital certificates be exchanged in the authentication phase. The server presents a certificate to the client and, after validating the server's certificate, the client presents a client certificate to the server for validation.
- LEAP is a pre-EAP, Cisco-proprietary protocol with many of the features of EAP protocols. Cisco controls the ability of other vendors to implement this protocol, so it should be selected for use only when limited brand choice for client, access-point and server products is not a concern. Once you've set up LEAP authentication, you need to enter the username and password of your computer.
- PEAP & TTLS are similar to, yet easier than, TLS in that they specify a stand-alone authentication protocol be used within an encrypted tunnel. TTLS supports any protocol within its tunnel, including CHAP, MSCHAP, MSCHAPv2

and PAP. PEAP specifies that an EAP-compliant authentication protocol must be used; this adapter supports MD5, TLS, GTC (Generic Token Card) and MSCHAPv2. That a client certificate be required for authentication is optional.

Tunnel: Options are MD5, GTC, TLS and MSCHAP-v2.
Username: This is the certificate username on the RADIUS server.
Identity: This is the user's identity on the RADIUS server.
Password: This is the user's password on the RADIUS server.
Certificate: Select the certificate for RADIUS server authentication.

2.3 Available Network

When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of your adapter, then automatically connect to the wireless network with the highest signal strength. On this screen, you can see all the nearby networks listed and you can change the connection to another network.



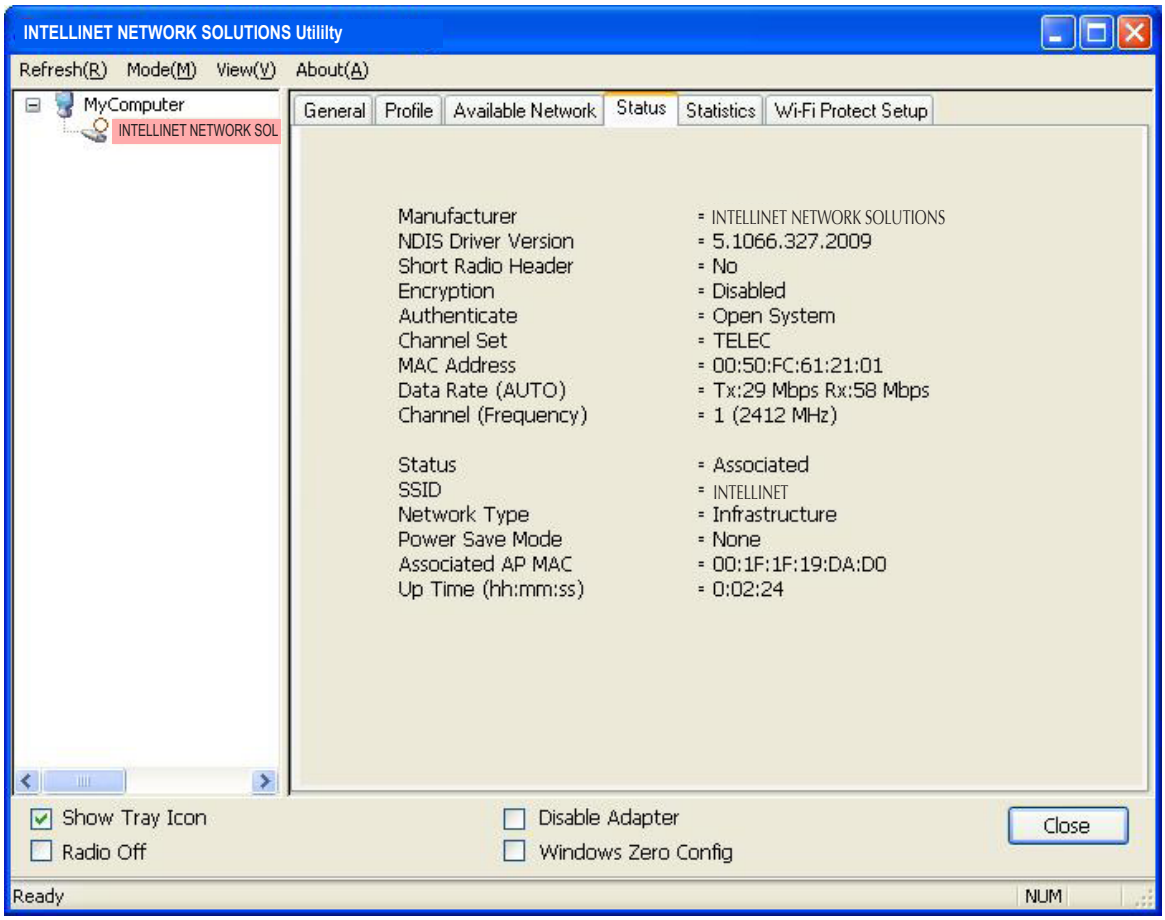
Available Network(s): This list presents important connection information about the available wireless networks within the range of your adapter. To connect to any network on the list, highlight it and double-click.

Refresh: Click to update the Available Network(s) list. It is recommended that the list be refreshed anytime a different network is selected.

Add to Profile: Click to add the selected network to a profile so you can connect to a previously joined network quicker (see 2.2 Profile).

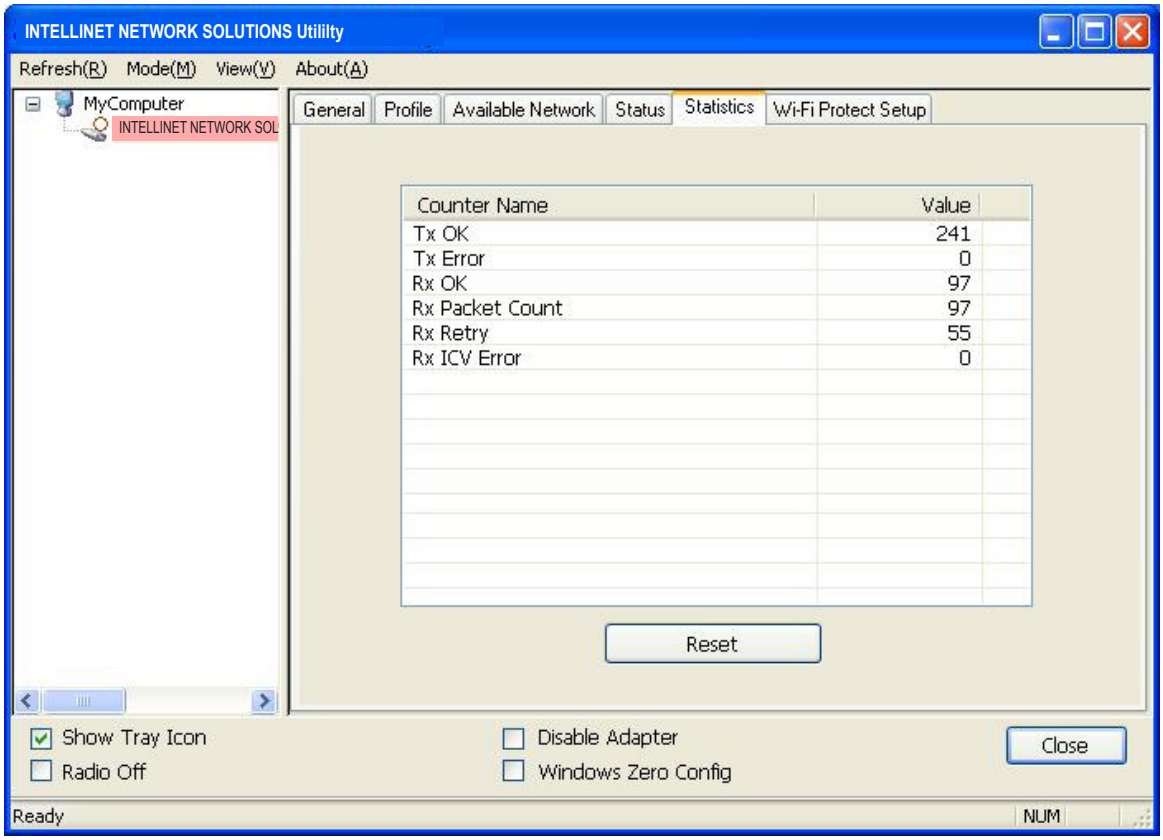
2.4 Status

This screen shows information about the manufacturer, driver version, settings of the wireless network the adapter is connecting to (helpful if you don't know this when you're trying to establish a connection), linking time and link status.



2.5 Statistics

You can get the real-time information about packet transmissions and the receiving status during wireless communications from this screen. To update the statistics values, click “Reset.”

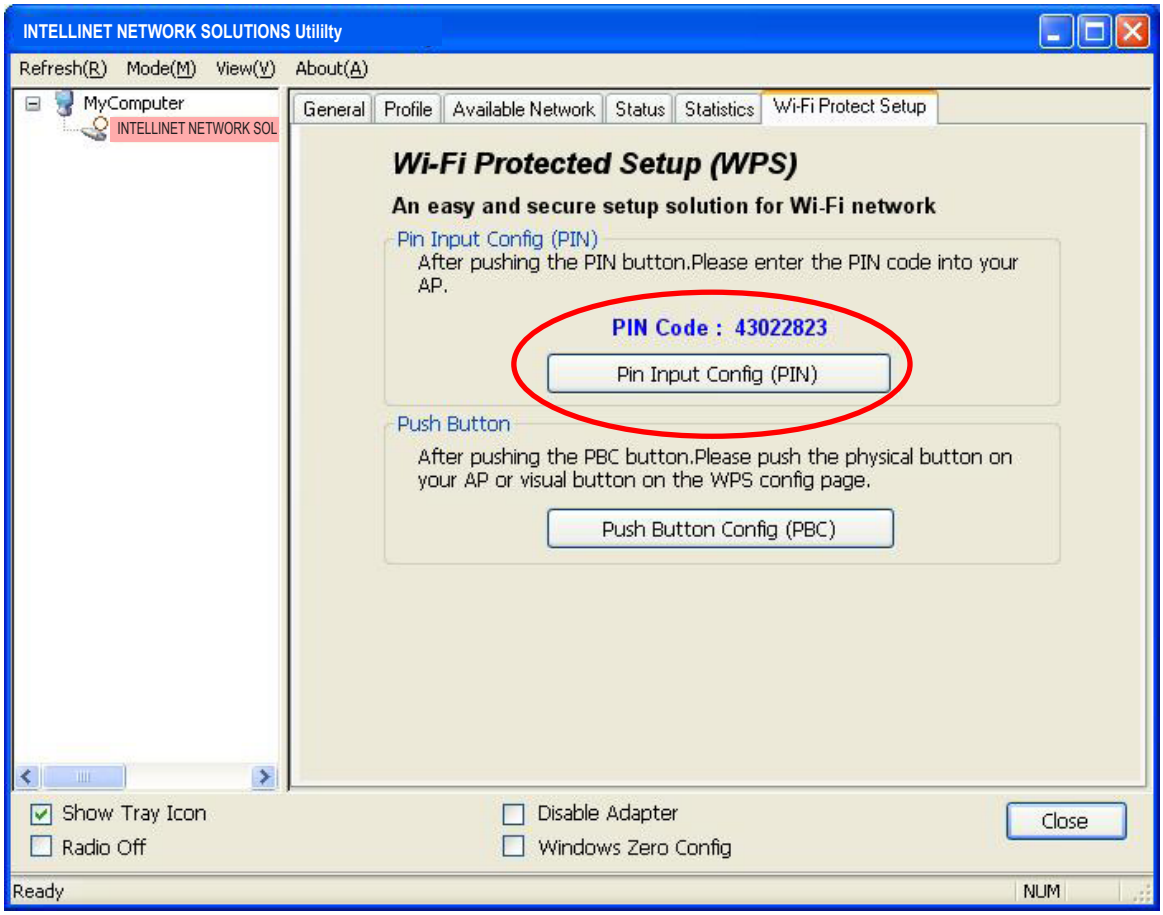


2.6 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is the latest wireless network technology and makes wireless network setup very simple. If you have a WPS-enabled wireless access point and you want to establish a secure connection to it, you don’t have to configure the wireless access point and set up data encryption all by yourself. All you need to do is go to this screen, click either “PBC” or “PIN,” then — on the wireless access point you want to connect to — either press the WPS button on the AP’s chassis or enter the eight-digit code found here on the adapter’s Configuration Utility Wi-Fi Protected Setup screen.

2.6.1 NETWORK SETUP USING PIN INPUT CONFIG (PIN)

1. Enter the PIN code of your wireless adapter (displayed right above the “PIN” button — see image below) on the wireless access point you want to connect to. If necessary, refer to the user manual of the wireless AP for instructions.


INTELLINET NETWORK SOLUTIONS Utility
Refresh(R) Mode(M) View(V) About(A)
MyComputer
INTELLINET NETWORK SOL
General Profile Available Network Status Statistics Wi-Fi Protect Setup
Wi-Fi Protected Setup (WPS)
An easy and secure setup solution for Wi-Fi network
Pin Input Config (PIN)
After pushing the PIN button.Please enter the PIN code into your AP.
PIN Code : 43022823
Pin Input Config (PIN)
Push Button
After pushing the PBC button.Please push the physical button on your AP or visual button on the WPS config page.
Push Button Config (PBC)
Show Tray Icon
Radio Off
Disable Adapter
Windows Zero Config
Close
Ready
NUM

2. Click “Pin Input Config (PIN)” and the prompt at right will display. Click “Yes” to select a specific wireless access point or click “No” to start the PIN method of WPS.

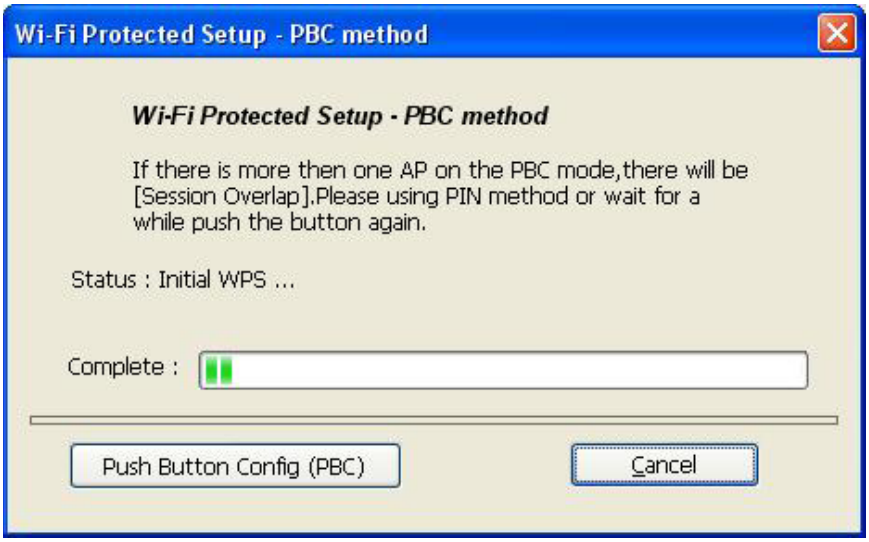
3. If you click “Yes,” the prompt at right will display. Select the wireless AP name you want to connect to and click “Select.”

4. A Status screen will display to indicate the progress of the procedure, which can take up to two minutes or so. If a wireless access point with the correct PIN code is found, you'll be connected to it.

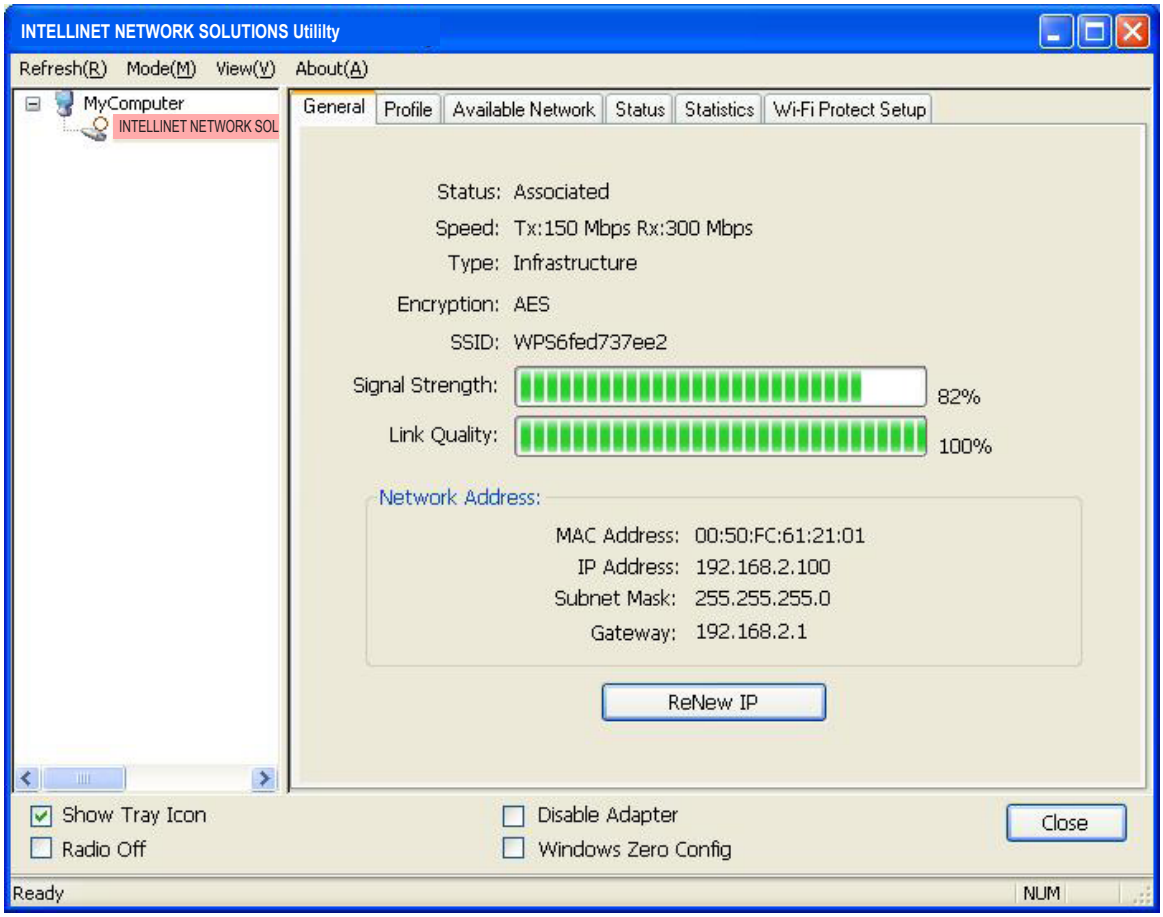
Wi-Fi Protected Setup - PIN method
Wi-Fi Protected Setup - PIN method
Please enter the following PIN code into your AP .
PIN Code : 98753420
Status : Initial WPS ...
Cancel

2.6.2 NETWORK SETUP USING PUSH BUTTON CONFIG (PBC)

1. Begin the PBC pairing procedure by setting up the access point. Refer to the user manual of the wireless AP for instructions. Click "Push Button Config (PBC)" on the Wi-Fi Protected Setup screen to begin the wireless connection using WPS. This procedure can take up to a minute to complete.


Wi-Fi Protected Setup - PBC method
Wi-Fi Protected Setup - PBC method
If there is more then one AP on the PBC mode,there will be [Session Overlap].Please using PIN method or wait for a while push the button again.
Status : Initial WPS ...
Complete :
Push Button Config (PBC)
Cancel

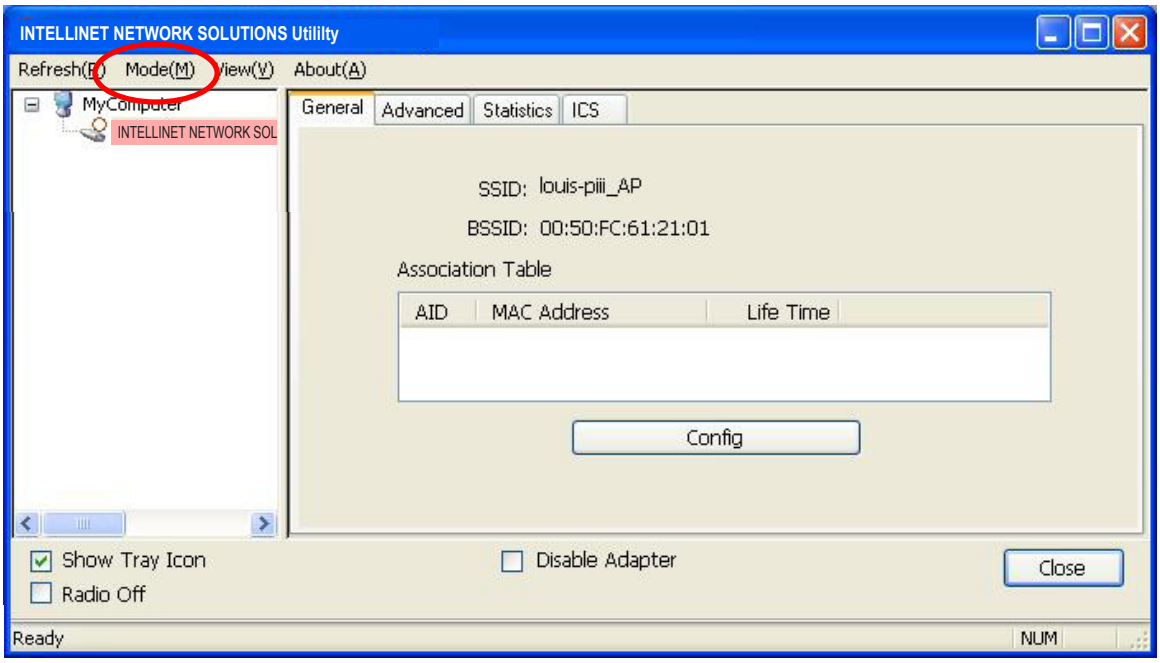
2. Once a successful WPS connection has been made between the wireless adapter and the access point, details about the connected access point will be displayed (as shown below).


INTELLINET NETWORK SOLUTIONS Utility
Refresh(R) Mode(M) View(V) About(A)
MyComputer
INTELLINET NETWORK SOL
General
Profile
Available Network
Status
Statistics
Wi-Fi Protect Setup
Status: Associated
Speed: Tx:150 Mbps Rx:300 Mbps
Type: Infrastructure
Encryption: AES
SSID: WPS6fed737ee2
Signal Strength:
82%
Link Quality:
100%
Network Address:
MAC Address: 00:50:FC:61:21:01
IP Address: 192.168.2.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.2.1
ReNew IP
Show Tray Icon
Radio Off
Disable Adapter
Windows Zero Config
Close
Ready
NUM

2.7 SoftAP

The Wireless 150N USB Mini Adapter can also be used as a wireless access point. On any of the menu screens, go to Mode(M) and select “Access Point.”

2.7.1 GENERAL



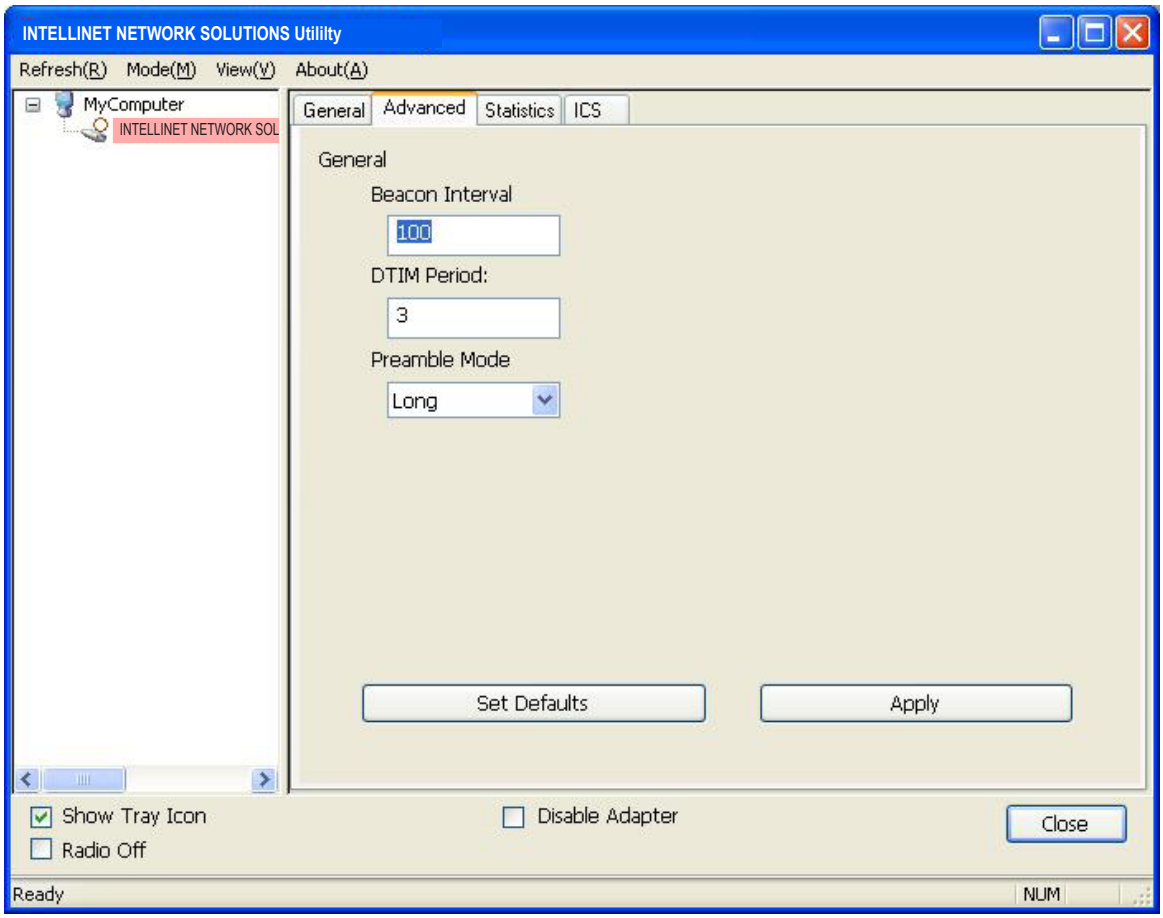
SSID: The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN that prevents unintentional merging of two co-located WLANs. The default SSID of the AP is <Full Computer Name> + “_AP.” Wireless adapters connected to the AP should set up the same SSID as the AP.

BSSID: This is the MAC address of the adapter.

Association Table: All wireless adapters connected to the software AP will be listed in the window.

Config: Click to access configuration options for the AP (shown at right). Refer to 2.2 Profile for details, and note that Ad Hoc mode is not enabled for the AP.

2.7.2 AP ADVANCED



Beacon Interval: Specify the duration between beacon packets (milliseconds). The range for the beacon period is 20-1000 milliseconds, with a typical value of 100.

DTIM Period: This is the sending interval of the AP's traffic broadcast. The default value is 3 beacons.

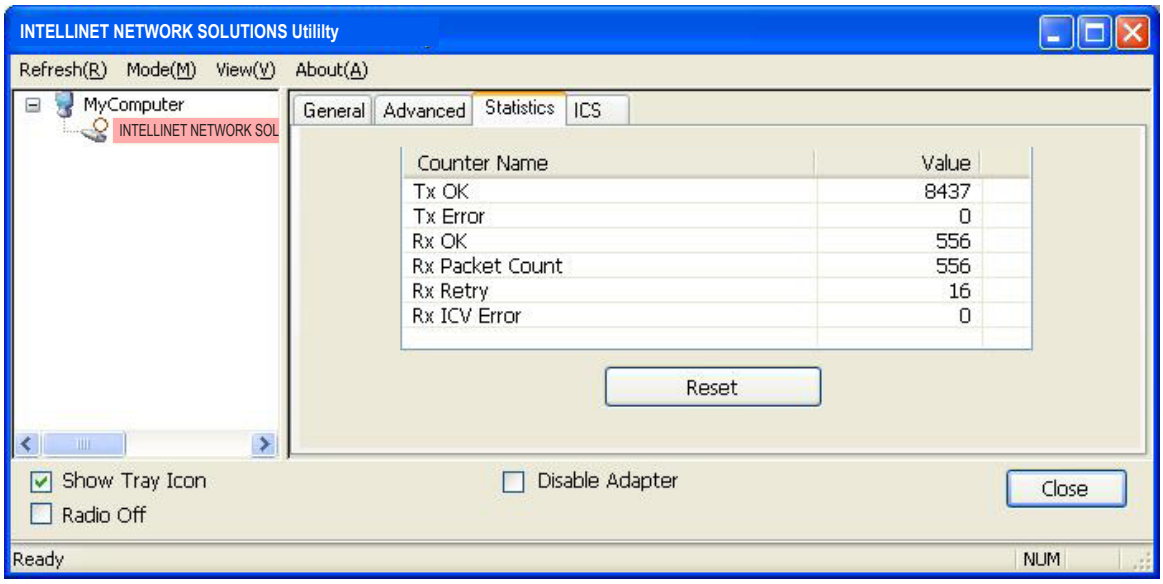
Preamble: This is the length ("Short" or "Long") of the CRC block for communication among wireless stations. High network traffic areas should use "Short."

Set Defaults: Click to return to default settings.

Apply: Click to confirm the settings.

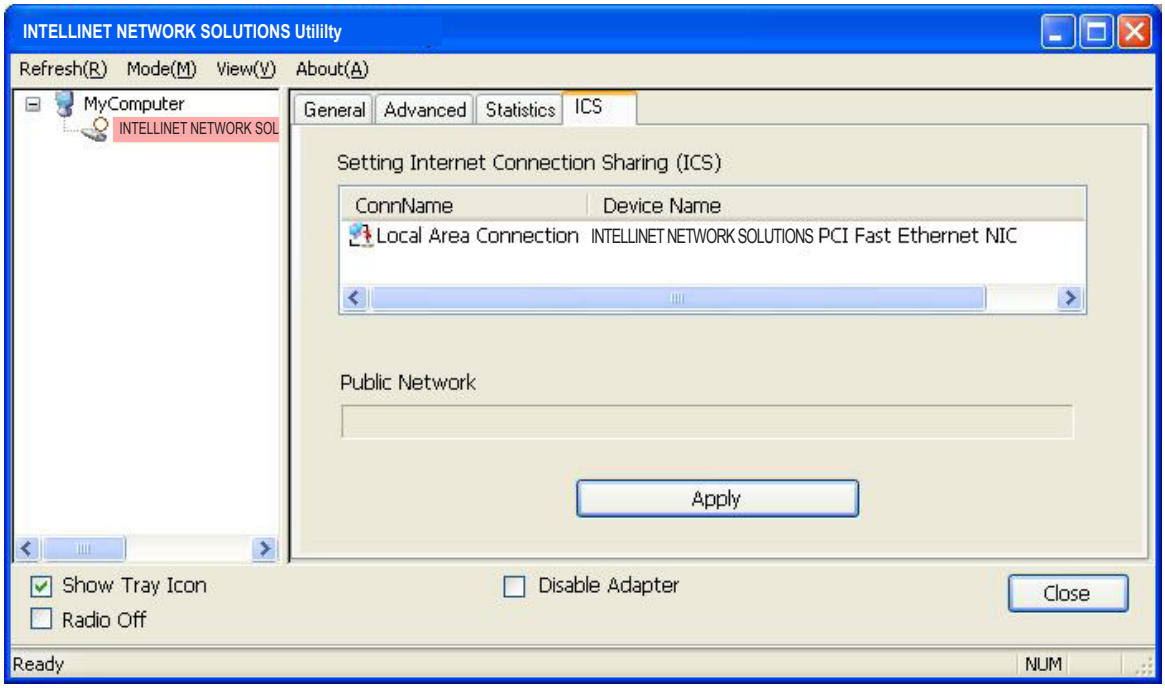
2.7.3 AP STATISTICS

You can get the real-time information about packet transmissions and the receiving status during wireless communications from this screen. To update the statistics values, click “Reset.”



2.7.4 ICS

To connect to the Internet through this adapter using SoftAP, you need to make a bridge between SoftAP and the Internet connection. Select the Internet connection and click “Apply.”



3 SPECIFICATIONS

Standards
- IEEE 802.11b (11 Mbps Wireless LAN)
- IEEE 802.11g (54 Mbps Wireless LAN)
- IEEE 802.11e (QoS Enhancement WMM)
- Upward compatible to IEEE 802.11n draft 2.0 (150 Mbps Wireless LAN)

General
- Interface: Hi-Speed USB 2.0
- Chipset: Realtek RTL8188SU
- Frequency band: 2.4000 – 2.483 GHz (Industrial Scientific Medical Band)
- Modulation technologies:
  - 802.11b: Direct Sequence Spread Spectrum (DSSS): DBPSK, DQPSK, CCK
  - 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
  - 802.11n: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
- Security:
  - 64/128-bit WEP data encryption
  - WPA and WPA2
  - Cisco CCX
- Transmit power:
  - 150 Mbps, 14 dBm +/- 1.5 dBm
  - 54 Mbps, 14 dBm +/- 1.5 dBm
  - 11 Mbps, 17 dBm +/- 1.5 dBm
- Certification: FCC Class B, CE

LEDs
- Link/Activity

Environmental
- Dimensions: 7 (H) x 15 (W) x 27 (L) mm (0.27 x 0.6 x 1.1 in.)
- Weight: 0.14 kg (0.3 lbs.)
- Operating temperature: 0 – 40°C (32 – 104°F)
- Operating humidity: 10 – 90% RH, non-condensing
- Storage temperature: -20 – 60°C (-4 – 149°F)

System Requirements
- Notebook or desktop PC with Pentium 1 GHz-compatible processor or higher
- Windows XP/Vista or Windows 7
- Available Hi-Speed USB 2.0 port

Package Contents
- Wireless 150N USB Mini Adapter
- Quick installation guide
- Setup CD and user manual

INTELLINET NETWORK SOLUTIONS™ offers a complete line
of active and passive networking products.
Ask your local computer dealer for more information or visit
www.intellinet-network.com.

Copyright © INTELLINET NETWORK SOLUTIONS
All products mentioned are trademarks or registered trademarks of their respective owners.